PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/761,697
Filing Date	1/20/04
First Named Inventor	Yuji Suga
Art Unit	2131
Examiner Name	
Attorney Docket Number	CFA00044US

Total Number of Pages in This Submission: 33

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☑ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance communication to Technology Center (TC)
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Canon U.S.A., Inc. IP Department Fidel Nwamu
Signature	Fidel Nwamu
Date	5/3/04

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Fidel Nwamu		
Signature	Fidel Nwamu	Date	5/3/04

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　１月２４日

出願番号
Application Number: 特願２００３－０１６７１８

[ST. 10/C]: [ＪＰ２００３－０１６７１８]

出願人
Applicant(s): キヤノン株式会社

２００４年　１月１４日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３１１１１４５

【書類名】　特許願
【整理番号】　251199
【提出日】　平成15年 1月24日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　7/00
【発明の名称】　連鎖型署名作成方法
【請求項の数】　1
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　須賀　祐治
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100076428
【弁理士】
【氏名又は名称】　大塚　康徳
【電話番号】　03-5276-3241
【選任した代理人】
【識別番号】　100112508
【弁理士】
【氏名又は名称】　高柳　司郎
【電話番号】　03-5276-3241
【選任した代理人】
【識別番号】　100115071
【弁理士】
【氏名又は名称】　大塚　康弘
【電話番号】　03-5276-3241

【選任した代理人】

【識別番号】　100116894

【弁理士】

【氏名又は名称】　木村　秀二

【電話番号】　03-5276-3241

【手数料の表示】

【予納台帳番号】　003458

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0102485

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　連鎖型署名作成方法

【特許請求の範囲】

【請求項１】　Ｎ個の公開鍵とそのうちの１つの公開鍵に対応する秘密鍵によって作成可能で、Ｎ個の公開鍵のそれぞれについて署名の検証が可能で、Ｎ人のメンバーのうち誰が署名したかを秘匿することのできる連鎖型署名において、前記連鎖型署名データの作成者以外のユーザが署名していないことを検証できるようにするための否認データを生成する工程を備えることを特徴とする連鎖型署名作成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は入力デジタルデータに対する連鎖型署名データを生成するために用いて好適なものである.

【従来の技術】

文書や画像データがインターネットなどの広域ネットワーク網を通して流通する場合、デジタルデータは改変が容易であるため、第三者によってデータが改ざんされる危険性がある。そこで、送信されてきたデータが改ざんされたかどうかを受信者が検出するために、改ざん防止用の付加データを検証する方式としてデジタル署名という技術が提案されている。デジタル署名技術は、データ改ざんだけではなく、インターネット上でのなりすまし、否認などを防止する効果も持ち合わせている。

【０００２】

[デジタル署名]

デジタル署名データ生成にはハッシュ関数と公開鍵暗号とが用いられる。これは、秘密鍵をＫｓ、公開鍵をＫｐとすれば、送信者は、入力データＭにハッシュ処理を施して固定長データＨ（Ｍ）を算出した後、秘密鍵Ｋｓで上記固定長データＨ（Ｍ）を変換してデジタル署名データＳを作成し、その後、デジタル署名データＳと入力データＭとを受信者に送信する。

【０００３】

受信者は、上記デジタル署名データＳを上記公開鍵Ｋｐで変換（復号）したデータと、入力データＭにハッシュ処理を施したデータとが一致するかどうか検証する。そして、上記検証の結果が一致していなければ、データＭの改ざんが行われたことを検出できる。

【０００４】

デジタル署名にはＲＳＡ、ＤＳＡなど公開鍵暗号方式が用いられおり、署名の安全性は、秘密鍵の所有者以外のエンティティは、署名を偽造、もしくは秘密鍵を解読することが離散対数問題に帰着され、計算量的に困難であることに基づいている。

【０００５】

［ハッシュ関数］

次に、ハッシュ関数について説明する。ハッシュ関数はデジタル署名データの生成を高速化するため等に用いられる。ハッシュ関数は任意の長さのデータＭに処理を行い、一定の長さの出力データを生成する機能を持っている。ここで、出力Ｈ（Ｍ）を平文データＭのハッシュデータと呼ぶ。

【０００６】

特に、一方向性ハッシュ関数は、データＭを与えた時、Ｈ（Ｍ’）＝Ｈ（Ｍ）となる平文データＭ’の算出が計算量的に困難であるという性質を持っている。上記一方向性ハッシュ関数としてはＭＤ２、ＭＤ５、ＳＨＡ－１などの標準的なアルゴリズムが存在しており、これらのアルゴリズムは公開されている。

【０００７】

［公開鍵暗号］

次に、公開鍵暗号について説明する。公開鍵暗号は２つの異なる鍵を利用し、片方の鍵で暗号処理したデータは、もう片方の鍵でしか復号処理できないという性質を持っている。上記２つの鍵のうち、一方の鍵は公開鍵と呼ばれ、広く公開するようにしている。また、もう片方の鍵は秘密鍵と呼ばれ、本人のみが持つ鍵である。

【０００８】

公開鍵暗号方式を用いたデジタル署名においては、次のように署名者を匿名にする技術が開発されている。ここでは、グループ署名とリング署名（連鎖型署名）について説明する。

【０００９】

［グループ署名］

グループ署名とは、署名がグループのメンバーにより作成されたかどうかを誰でも検証できるが、誰が署名したかはわからない署名方式であり、1991年にChaumによって提案された方式である。メンバーのほかに特権を持つ管理者が存在し、問題が起こったときは、特別な方法で署名者を特定できる仕組みを備えている。

【００１０】

グループ署名は、ａ）グループ公開鍵がグループに所属するメンバーの公開鍵のリストとなっている公開鍵登録型と、ｂ）グループメンバに対しメンバーである証明書を発行する証明書発行型の2つに大別することができる。

【００１１】

ａ）の手法ではグループ公開鍵と署名のサイズがメンバー数に依存した大きさとなり非効率である。しかしグループからメンバーを削除するのは容易に行うことができる。

【００１２】

ｂ）の手法はグループ公開鍵と署名のサイズはメンバー数に依存しないが、メンバーの削除を行うには一度発行した証明書を無効にする必要があるという特徴を持つ。

【００１３】

グループ署名は、利用者のプライバシーを保護する目的のアプリケーションである、電子決済プロトコルや、電子オークションプロトコルに応用されている。

［リング署名］

グループ署名方式では自分の身元を明かすことなくグループへの所属を証明することができるが、メンバーとは別に特権を持つ管理者を必要としていた。一方、リング署名は、このような管理者は必要なく、署名作成のためのメンバーとの

事前やり取りなどは全く必要のない方式で、２００１年にＳｈａｍｉｒらによって提案された。

【００１４】

［Ｓｈａｍｉｒらによるリング署名］

｛0，1｝ ｌの入出力を持つ落とし戸付き一方向性置換関数をｇ＿0，…，ｇ＿（ｎ－１）とする。Ｈ（）は通常のハッシュ関数、Ｅ＿Ｋ（）、Ｄ＿Ｋ（）を共有鍵Ｋによる共通鍵暗号の暗号化関数、復号化関数とする。署名作成者はあるｉにおけるｇ＿ｉの逆関数を秘密に保持しているとする。ここでｘｏｒは排他的論理和演算のことである。

【００１５】

［Ｓｈａｍｉｒリング署名：署名作成］　　文書Mに対する署名の作成手順

１）　Ｋ：＝Ｈ（Ｍ）とおく。

【００１６】

２）　Ｚ＿0を｛0，1｝ ｌから任意に選択する。

【００１７】

３）　ｊ＝0，…，ｉ－１（昇順）について、以下を繰り返す。ｒ＿ｊを｛0，1｝ ｌから任意に選択し、ｙ＿ｊ：＝ｇ＿ｊ（ｒ＿ｊ）、ｚ’＿ｊ：＝ｚ＿ｊ　ｘｏｒ　ｙ＿ｊ，ｚ＿（ｊ＋１）：＝Ｅ＿Ｋ（ｚ’＿ｊ）とおく。

【００１８】

４）　ｚ’＿（ｎ＋１）：＝Ｄ＿Ｋ（Ｚ＿0）

５）　ｊ＝ｎ－１，…ｉ＋１（降順）について以下を繰り返す。ｒ＿ｊを｛0，1｝ ｌから任意に選択し、ｙ＿ｊ：＝ｇ＿ｊ（ｒ＿ｊ）、ｚ＿ｊ：＝ｚ’＿ｊ　ｘｏｒ　ｙ＿ｊ，ｚ＿（ｊ－１）：＝Ｄ＿Ｋ（ｚ’＿ｊ）とおく。

【００１９】

６）　ｇ＿ｉの逆関数を知る署名者が、以下を計算する。ｙ＿ｉ：＝ｚ＿ｉ　ｘｏｒ　ｚ’＿ｉ，ｒ＿ｉ：＝ｇ＿ｉ－１（ｙ＿ｉ）

７）　署名（ｚ＿0，ｒ＿0，ｒ＿1，…，ｒ＿（ｎ－１））を出力する。

【００２０】

［Ｓｈａｍｉｒリング署名：署名検証］　　文書Mに対する署名（ｚ＿0，ｒ

＿０，ｒ＿１，…，ｒ＿（ｎ－１））の検証手順

１）　Ｋ：＝Ｈ（Ｍ）とおく。

【００２１】

２）　ｊ＝０，…，ｎ－１（昇順）について、以下を繰り返す。ｙ＿ｊ：＝ｇ＿ｊ（ｒ＿ｊ）、ｚ’＿ｊ：＝ｚ＿ｊ　ｘｏｒ　ｙ＿ｊ，ｚ＿（ｊ＋１）：＝Ｅ＿Ｋ（ｚ’＿ｊ）とおく。

【００２２】

３）　ｚ＿ｎ＝ｚ＿０かどうかを検証する。

【００２３】

以上の手順では、様々な既存の署名方式に適用できる点が優れているが、ａ）落とし戸付き一方向性置換関数、ｂ）共有鍵暗号、復号関数の２つが安全に提供されねばならない。

【００２４】

［大久保らによるリング署名］

上記の問題を解決するために、ａ）、ｂ）の関数を必要としない署名方法が提案されている。ただし、Ｓｃｈｎｏｒｒ署名と呼ばれる既存の署名方式にのみ適用できる点で汎用性が低い。

【００２５】

［Ｓｃｈｎｏｒｒ署名］

従来技術としてのＳｃｈｎｏｒｒ署名を説明する（例えば、非特許文献１を参照）。

【００２６】

ｐ，ｑを素数とし、ｐ－１はｑを割り切るとする。ｇをＺ＿ｐ＊（位数ｐの巡回群Ｚ＿ｐから０を省いた乗法群）から任意に選択した、位数ｑの元（生成元）とする。Ｚ＿ｐ＊から選択したｘを秘密鍵とし、それに対する公開鍵ｙをｙ：＝g^x　ｍｏｄ　ｐとおく。Ｈ（）をハッシュ関数とする。

【００２７】

［Ｓｃｈｎｏｒｒ署名作成］　　文書Ｍに対する署名の作成手順

１）　αをＺ＿ｑから任意に選択し、Ｔ：＝g^{α}　ｍｏｄ　ｐとおく。

【００２８】

２）　ｃ：＝Ｈ（Ｍ｜｜Ｔ）とおく。ただし｜｜はデータの連結を意味する。

【００２９】

３）　ｓ：＝α－ｘｃ　ｍｏｄ　ｑとおき、（ｓ，ｃ）を署名データとする。

【００３０】

［Ｓｃｈｎｏｒｒ署名検証］　　文書Ｍに対する署名（ｓ，ｃ）の検証手順

Ｔ：＝ｇ^{s}ｙ^{c}　ｍｏｄ　ｐとおき、ｃ＝Ｈ（Ｍ　｜｜　Ｔ）かどうか検証する。

【００３１】

大久保らによるリング署名は、Schnorr署名を逐次的に結合したものと捉えることができる。

【００３２】

以下、従来技術としてのＳｃｈｎｏｒｒ署名によるリング署名を説明する（例えば、非特許文献２を参照）。

【００３３】

記号の表記方法はＳｃｈｎｏｒｒ署名での記号に準じる。署名者は、ｎ個の公開鍵（ｇ＿ｉ，ｐ＿ｉ，ｑ＿ｉに対する）ｙ＿ｉを得ておく。そのうち、ｙ＿ｉに対する秘密鍵ｘ＿ｉを知っているものとする。Ｈ＿ｉ（）はハッシュ関数とする。添字はｍｏｄ　ｎと取るものとする。例えばｘ＿（ｎ＋１）はｘ＿０とみなす。

【００３４】

［Ｓｃｈｎｏｒｒリング署名作成］　　文書Ｍに対する署名の作成手順

１）　αをＺ＿（ｑ＿ｉ）から任意に選択し、Ｔ＿ｉ：＝ｇ＿ｉ$^{\alpha}$　ｍｏｄ　ｐ＿ｉとおく。

【００３５】

２）　ｃ＿（ｉ＋１）：＝Ｈ（Ｍ｜｜Ｔ＿ｉ）とおく。

【００３６】

３）　ｊ＝ｉ＋１，…，ｉ－１（昇順）について、以下を繰り返す。ｓ＿ｊをＺ＿（ｑ＿ｊ）から任意に選択し、Ｔ＿ｊ：＝ｇ＿ｊ^{s_j}ｙ＿ｊ^{c_j}　ｍｏ

ｄ　ｐ＿ｊ，ｃ＿（ｊ＋１）：＝Ｈ（Ｍ｜｜Ｔ＿ｊ）とおく。

【００３７】

４）　ｓ＿ｉ：＝α－ｘ＿ｉ　ｃ＿ｉ　ｍｏｄ　ｑ＿ｉとおき、（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））を署名データとする。

【００３８】

［Ｓｃｈｎｏｒｒリング署名検証］　文書Ｍに対する署名（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））の検証手順

１）　ｊ＝０，…，ｎ－１（昇順）について、以下を繰り返す。Ｔ＿ｊ：＝ｇ＿ｊｓ＿ｊｙ＿ｊｃ＿ｊ　ｍｏｄ　ｐ＿ｊ，ｃ＿（ｊ＋１）：＝Ｈ（Ｍ｜｜Ｔ＿ｊ）とおく。

【００３９】

２）　ｃ＿ｎ＝ｃ＿０かどうかを検証する。

【非特許文献１】

C.P.Schnorr, Eficient Signature Generation by Smart Cards", Journal of Cryptology, Vol.4, No.3, pp.161-174 (1991)

【非特許文献２】

大久保,安部,鈴木,辻井, “証明長が短い 1-out-of-n 証明”, 4C-4, pp.189-193, 2002年 暗号と情報セキュリティシンポジウム(SCIS200)

【００４０】

【発明が解決しようとする課題】

Ｓｈａｍｉｒらによるリング署名、大久保らによるＳｃｈｎｏｒｒリング署名は、管理者不在であることにより、自由に第３者の公開鍵を取得して、擬似的に署名を施すことで、匿名性を確保している。しかし、第３者の公開鍵を取得するだけでリングの中に擬似的な署名を含めることができるため、勝手に公開鍵を流用される可能性がある。この場合、勝手に流用された公開鍵に対する秘密鍵を保持するユーザは、自らが署名していないことを示す（否認する）ことができない問題が生じる。

【００４１】

リング署名の具体的な適用例としては、報道機関に対する内部告発が挙げられ

る。告発者は自分の身元を明かすことなく、文書の信憑性を確保することができる意味で有用である。しかし、告発者以外のリング署名内に含まれた者は、実際に告発していないにも関わらず疑いをかけられてしまう可能性がある。この場合、「自らが署名した文書ではない」ことを第３者に証明する手立てはない。

【００４２】

本発明は以上の問題に鑑みてなされたものであり、リング署名において、勝手に流用された公開鍵に対する秘密鍵を保持するユーザ自身が署名を作成していないことを示す否認データを作成することを目的とする。

【００４３】

また、この否認データは、リング署名の署名者は作成することができないようにする必要がある。前述の例では、実際に告発したにも関わらず、「自らが署名した文書ではない」ことを第３者に証明することが可能であると、否認していない者が疑いをかけられてしまうことになる。

【００４４】

そのため、本発明の別の目的としては、否認データは、リング署名の署名者は作成することができないようにすることを目的とする。

【００４５】

【課題を解決するための手段】

本発明の目的を達成するために、例えば本発明の連鎖型署名作成方法は以下の構成を備える。

【００４６】

すなわち、Ｎ個の公開鍵とそのうちの１つの公開鍵に対応する秘密鍵によって作成可能で、Ｎ個の公開鍵のそれぞれについて署名の検証が可能で、Ｎ人のメンバーのうち誰が署名したかを秘匿することのできる連鎖型署名において、前記連鎖型署名データの作成者以外のユーザが署名していないことを検証できるようにするための否認データを生成する工程を備えることを特徴とする。

【００４７】

【発明の実施の形態】

以下添付図面を参照して、本発明を好適な実施形態に従って詳細に説明する。

【００４８】

［第１の実施形態］

本実施形態に係る連鎖型署名作成処理、連鎖型署名検証処理を実行する装置には例えば図１に示す基本構成を備えるコンピュータが適用できる。以下、このコンピュータの基本構成について図１を参照して説明する。

【００４９】

すなわち、コンピュータ１００は図１に示すように、公衆回線等のモデム１１８、表示部としてのモニタ１０２、ＣＰＵ１０３、ＲＯＭ１０４、ＲＡＭ１０５、ＨＤＤ（ハードディスクドライブ）１０６、ネットワークへのネットワーク接続部１０７、ＣＤ－ＲＯＭドライブ１０８、ＦＤ（フレキシブルディスク）ドライブ１０９、ＤＶＤ（デジタル・ビデオ・ディスク、またはDigital Versatile Disk）－ＲＯＭドライブ１１０、プリンタ１１５のインターフェース（Ｉ／Ｆ）１１７、及び操作部としてのマウス１１２やキーボード１１３等のインターフェース（Ｉ／Ｆ）１１１が、バス１１６を介して互いに通信可能に接続されて構成されている。

【００５０】

マウス１１２及びキーボード１１３は、コンピュータ１００に対する各種指示等をユーザが入力するための操作部である。この操作部を介して入力された情報（操作情報）は、インターフェース１１１を介して、ＣＰＵ１０３に通知される。

【００５１】

コンピュータ１００内に保持されている各種情報（文字情報や画像情報等）は、プリンタ１１５により印刷出力できるようになされている。

【００５２】

モニタ１０２はＤＲＴや液晶画面などにより構成されており、ユーザへの各種指示情報や、文字情報或いは画像情報等の各種情報の表示を行う。

【００５３】

ＣＰＵ１０３は、コンピュータ１００全体の動作制御を司るものであり、以下説明する連鎖型署名作成処理、連鎖型署名検証処理を実行するものである。ＣＰ

Ｕ１０３は、ＨＤＤ１０６やＣＤ－ＲＯＭドライブ１０８、ＦＤドライブ１０９、ＤＶＤ－ＲＯＭドライブ１１０等からＲＡＭ１０５にロードされた各種の処理プログラム（ソフトウェアプログラム）を実行することで、各種の処理を行う。

【００５４】

ＲＯＭ１０４は、署名の作成・検証処理のための処理プログラム等の各種処理プログラムや、各種データ等を記憶する。

【００５５】

ＲＡＭ１０５は、ＣＰＵ１０３での各種処理のために、一時的に処理プログラムや処理対象の情報を格納するための作業用エリア等を備えるメモリである。

【００５６】

ＨＤＤ１０６は、大容量記憶装置の一例としての構成要素であり、文字情報や画像情報、或いは各種処理の実行時にＲＡＭ１０５等へ転送される情報変換処理等のための処理プログラム等を保存する。

【００５７】

ＣＤ－ＲＯＭドライブ１０８は、外部記憶媒体の一例としてのＣＤ－ＲＯＭ（ＣＤ－Ｒ）に記憶されたデータを読み込み、また、ＣＤ－Ｒへデータを書き出す機能を有する。

【００５８】

ＦＤドライブ１０９は、外部記憶媒体の一例としてのＦＤ（フレキシブルディスク）に記憶されたデータを読み出す。また、種々のデータをＦＤへ書き込む機能を有している。

【００５９】

ＤＶＤ－ＲＯＭドライブ１１０は、外部記憶媒体の一例としてのＤＶＤに記憶されたデータを読み出し、また、ＤＶＤへデータを書き込む機能を有している。

【００６０】

なお、ＣＤ、ＦＤ、ＤＶＤ等の外部記憶媒体に対して、例えば、編集用のプログラム或いはプリンタドライバが記憶されている場合には、これらのプログラムをＨＤＤ１０６へインストールしておき、必要に応じて、ＲＡＭ１０５へ転送するように構成してもよい。

【００６１】

インターフェース（Ｉ／Ｆ）１１１は、マウス１１２或いはキーボード１１３によるユーザからの入力を受け付けるためのものである。

【００６２】

モデム１１８は、通信モデムであり、インターフェース（Ｉ／Ｆ）１１９を介して、例えば、公衆回線等を通じて外部のネットワークに接続される。

【００６３】

ネットワーク接続部１０７は、インターフェース（Ｉ／Ｆ）１１４を介して、外部のネットワークに接続される。

【００６４】

以上の構成を備えるコンピュータによって、本実施形態に係る連鎖型署名作成処理、連鎖型署名検証処理を実行するが、夫々の処理を実行する装置は同一のものであっても良いし、別個の装置であっても良い。

【００６５】

次に、リング署名に対する否認データ作成処理について説明する。

【００６６】

［否認データ作成］　　Ｓｃｈｎｏｒｒリング署名に対する否認データの作成手順

否認データ作成者は、公開鍵ｙ＿ｉに対する秘密鍵ｘ＿ｉを保持するとする。

【００６７】

１）　α＊：＝ｓ＿ｉ＋ｘ＿ｉ　ｃ＿ｉとおく。

【００６８】

２）　ｒをＺ＿（ｑ＿ｉ）から任意に選択し、Ｔ＊：＝ｇ＿ｉ^{r}とおく。ｃ＿ｉ＊：＝Ｈ（Ｍ　｜｜　Ｔ＊　｜｜　Ｔ＿（ｉ－１）　｜｜　Ｒｅｐ）とおく。ここでＲｅｐは否認する趣旨が記述された誓約データである。

【００６９】

３）　ｓ＿ｉ＊：＝ｒ－α＊ｃ＿ｉ＊　ｍｏｄ　ｑ＿ｉとおき、リング署名（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））に対する否認データ（ｓ＿ｉ＊，ｃ＿ｉ＊）を作成する。

【００７０】

［否認データ検証］　　Ｓｃｈｎｏｒｒリング署名に対する否認データの検証手順

否認データ（ｓ＿ｉ＊，ｃ＿ｉ＊）に対し、Ｔ＊：＝　ｇ＿ｉｓ＿ｉ＊（Ｔ＿ｉ）ｃ＿ｉ＊　ｍｏｄ　ｐ＿ｉとおき、ｃ＿ｉ＊＝Ｈ（Ｍ　｜｜　Ｔ＊　｜｜　Ｔ＿（ｉ－１）　｜｜　Ｒｅｐ）が成立するか検証する。

【００７１】

図２は、リング署名に対する否認データ作成処理を行うための装置の機能構成、もしくはこの処理をコンピュータに実行させるためのプログラムの機能構成を示す図である。本実施形態では同図に示した各部の機能をプログラムにより表現し、このプログラムをコンピュータ１００に読み込ませることで、コンピュータ１００に同処理を行わせる。

【００７２】

否認データ作成者は、公開鍵ｙ＿ｉに対する秘密鍵ｘ＿ｉをコンピュータ１００に接続されたＨＤＤ１０６やＣＤ－ＲＯＭ、ＦＤ、ＤＶＤ－ＲＯＭ等に保持させておき、必要に応じてＲＡＭ１０５にロード可能なようにしておく。

【００７３】

上記［否認データ作成］の第１の処理を行うために、リング署名データＳが入力され、付随データ抽出モジュール２０４においてリング署名データＳからｓ＿ｉ，ｃ＿ｉを抽出する。抽出されたｓ＿ｉ，ｃ＿ｉ及び上記ｘ＿ｉから、α＊：＝ｓ＿ｉ＋ｘ＿ｉ　ｃ＿ｉを計算する。

【００７４】

上記［否認データ作成］の第２の処理を行うために、ｒをＺ＿（ｑ＿ｉ）から任意に選択し、Ｔ＊：＝ｇ＿ｉ^{r}を計算し、被署名データＭが入力され、同時に付随データ抽出モジュール２０４においてＴ＿（ｉ－１）が抽出され、次に誓約データ添付モジュール２０３において、被署名データＭに対して、Ｔ＿（ｉ－１）と誓約データＲｅｐが付加され、ハッシュ再計算モジュール２０５に渡され、ｃ＿ｉ＊：＝Ｈ（Ｍ　｜｜　Ｔ＊　｜｜　Ｔ＿（ｉ－１）　｜｜　Ｒｅｐ）を計算する。ここでＲｅｐは否認する趣旨が記述された誓約データである。

【００７５】

上記［否認データ作成］の第３の処理を行うために、付随データ抽出モジュール２０４から得たα＊およびハッシュ再計算モジュール２０５から得たｃ＿ｉ＊に基づき、再署名モジュール２０６にてｓ＿ｉ＊：＝ｒ－α＊　ｃ＿ｉ＊　ｍｏｄ　ｑ＿ｉを計算し、結果として否認データＲ＝（ｓ＿ｉ＊，ｃ＿ｉ＊）が出力される。

【００７６】

図３は否認データを作成する処理のフローチャートである。各ステップにおける処理は上述の通りであるので、ここでの説明は簡単なものにする。また、同図のフローチャートに従ったプログラムはＨＤＤ１０６やＣＤ－ＲＯＭドライブ１０８、ＦＤドライブ１０９、ＤＶＤ－ＲＯＭドライブ１１０等からＲＡＭ１０５にロードされ、ＣＰＵ１０３がこれを実行することで、コンピュータ１００は同図のフローチャートに従った処理、すなわち、否認データを作成する処理を実行することができる。

【００７７】

付随データ抽出モジュール２０４はステップＳ３０１における付随データの抽出処理を行い、誓約データ添付モジュール２０３はステップＳ３０２における誓約データの添付処理を行い、ハッシュ再計算モジュール２０５はステップＳ３０３におけるハッシュ再計算処理を行い、再署名モジュール２０６はステップＳ３０４における署名の再計算処理を行う。

【００７８】

リング署名（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））の中に含まれている偽造された署名ｓ＿ｉをｓ＿ｉ＊で置き換えることで否認を宣言している。このｓ＿ｉ＊を生成する操作は、公開鍵ｙ＿ｉに対する秘密鍵ｘ＿ｉを保持している者にしか作成できない。なぜならば、上記［否認データ作成］における第１の処理は、秘密鍵ｘ＿ｉを保持する者しか計算できず、また第３の処理は通常の署名操作と同一であり、秘密データα＊を保持する者しか計算できないためである。

【００７９】

また本実施形態では、ｃ＿ｉ＊の計算においてハッシュ関数に渡すデータとしてＴ＿（ｉ－１）やＲｅｐを含んでいるが、これらが包含されることは必須ではなく、第１の処理で得られたα＊を用いて再署名を施すことが安全性の根拠となる。したがってｃ＿ｉ＊の計算には何をハッシュ計算の対象とするかは他にもあらゆるバリエーションが容易に考えられる。

【００８０】

［第２の実施形態］

第１の実施形態では、作成された否認データをオフラインで検証する方式であったが、本実施形態では、インタラクティブに否認するプロトコルについて示す。

【００８１】

［否認するユーザＵとそれを検証するユーザＶの間のプロトコル］

１）　Ｖ→Ｕ：　リング署名（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））、チャレンジデータｒを送付。

【００８２】

２）　Ｕ→Ｖ：　以下のように計算されたｓ＿ｉ＊を送付。リング署名データからｓ＿ｉ，ｃ＿ｉを抽出し、α＊：＝ｓ＿ｉ＋ｘ＿ｉ　ｃ＿ｉとおき、ｃ＿ｉ＊：＝Ｈ（Ｍ　｜｜　Ｔ＊　｜｜　Ｔ＿（ｉ－１）　｜｜　ｒ）に対し、ｓ＿ｉ＊：＝ｒ－α＊　ｃ＿ｉ＊　ｍｏｄ　ｑ＿ｉを計算する。

【００８３】

３）　Ｖ：ｃ＿ｉ＊：＝Ｈ（Ｍ　｜｜　Ｔ＊　｜｜　Ｔ＿（ｉ－１）　｜｜　ｒ）に対し、ｃ＿ｉ＊＝Ｈ（Ｍ　｜｜　Ｔ＊　｜｜　Ｔ＿（ｉ－１）　｜｜　Ｒｅｐ）が成立するかどうかを検証する。検証ＯＫであれば、ユーザＵは、リング署名の作成者ではないことを証明したことになる。

【００８４】

図４は、上記プロトコルの処理を表す図である。ステップＳ４０１では上記プロトコル１）の処理を、ステップＳ４０２、Ｓ４０３では上記プロトコル２）の処理を、ステップＳ４０４では上記プロトコル３）の処理を行っている。

【００８５】

さらに、上記プロトコルではｓ＿ｉ＊が通信上流れるが、ゼロ知識証明プロトコルを用いて対話的に証明する方法でもよい。具体的には、α＊を計算できるのは秘密鍵ｘ＿ｉを保持している者だけであるので、ｇ＾（α＊）を公開し、それに対応するα＊を持っているかどうかを対話的に証明すればよい。

【００８６】

[第３の実施形態]

上記実施形態においては、Ｓｃｈｎｏｒｒ署名に対するリング署名をベースにしていたが、本実施形態ではＤＳＡ署名に対する拡張例を示す。この拡張方法は他の既存の署名方式に対しても適用できる。

【００８７】

[ＤＳＡ署名]

Federal Information Processing Standards (FIPS) 186-2, Digital Signature Standard (DSS), January 2000に記載の方式を説明する。記号の表記方法はＳｃｈｎｏｒｒ署名での記号に準じる。

【００８８】

[ＤＳＡ署名作成]　　文書Ｍに対する署名の作成手順

１）　αをＺ＿ｑから任意に選択し、Ｔ：＝（ｇ^α　ｍｏｄ　ｐ）　ｍｏｄ　ｑとおく。

【００８９】

２）　ｃ：＝Ｈ（Ｍ）とおく。

【００９０】

３）　ｓ：＝α^－１（ｃ＋ｘＴ）　ｍｏｄ　ｑとおき、（ｓ，Ｔ）を署名データとする。

【００９１】

[ＤＳＡ署名検証]　　文書Ｍに対する署名（ｓ，Ｔ）の検証手順

Ｔ＝（ｇｈ（Ｍ）ｓ＾－１ｙＴｓ＾－１　ｍｏｄ　ｐ）　ｍｏｄ　ｑかどうか検証する。

【００９２】

[ＤＳＡリング署名作成]　　文書Ｍに対する署名の作成手順

１）　Ｚ＿（ｑ＿ｉ）から任意に選択し、Ｔ＿ｉ：＝（ｇ＿ｉ$^{\alpha}$　ｍｏｄ　ｐ＿ｉ）　ｍｏｄ　ｑ＿ｉとおく。

【００９３】

２）　ｃ＿（ｉ＋１）：＝Ｈ（Ｍ　｜｜　Ｔ＿ｉ）とおく。

【００９４】

３）　ｊ＝ｉ＋１，…，ｉ－１（昇順）について、以下を繰り返す。ｓ＿ｊをＺ＿（ｑ＿ｊ）から任意に選択し、Ｔ＿ｊ：＝ｇ＿ｊ$^{c_j\,s_j\hat{}-1}$ｙ＿ｊ$^{T_j\,s_j\hat{}-1}$　ｍｏｄ　ｐ＿ｊ，ｃ＿（ｊ＋１）：＝Ｈ（Ｍ　｜｜　Ｔ＿ｊ）とおく。

【００９５】

４）　ｓ＿ｉ：＝α^{-1}（ｃ＿ｉ＋ｘ＿ｉ　Ｔ＿ｉ）　ｍｏｄ　ｑとおき、（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））を署名データとする。

【００９６】

［ＤＳＡリング署名検証］　　文書Ｍに対する署名（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））の検証手順

１）　ｊ＝０，…，ｎ－１（昇順）について、以下を繰り返す。Ｔ＿ｊ：＝ｇ＿ｊ$^{c_j\,s_j\hat{}-1}$ｙ＿ｊ$^{T_j\,s_j\hat{}-1}$　ｍｏｄ　ｐ＿ｊ，ｃ＿（ｊ＋１）：＝Ｈ（Ｍ　｜｜　Ｔ＿ｊ）とおく。

【００９７】

２）　ｃ＿ｎ＝ｃ＿０かどうかを検証する。

【００９８】

上記の方法のほかにも、ｃ＿ｉを連鎖させるのではなく、Ｔ＿ｉを連鎖させる方法でも実現可能である。

【００９９】

［第４の実施形態］

上記実施形態では誓約データＲｅｐを必要としていたが、事前計算データＴ＿ｊで代用する例を示す。第１の実施形態における［否認データ作成］の第２の操作において、ｃ＿ｉ＊：＝Ｈ（Ｍ　｜｜　Ｔ＿（ｉ－１）　｜｜　Ｒｅｐ）の代わりに、Ｒｅｐを使用しないで、ｃ＿ｉ＊：＝Ｈ（Ｍ　｜｜　Ｔ＿（ｉ－２））

などのようにＴ＿ｊ（ｊ≠ｉ）を用いることも可能である。

【０１００】

さらに、同じメッセージに対する連鎖型署名を複数作成し、ハッシュ対象データに先に生成した連鎖型署名データを含めることも可能である。たとえば２つの連鎖型署名を作成する際に、まずＨ（Ｍ　||　Ｔ＿ｉ　||　Ｒｅｐ）などとＲｅｐもハッシュ対象にした第１の連鎖型署名データ（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））を作成する。次にＲ＿１：＝Ｈ（（ｃ＿０，ｓ＿０，ｓ＿１，…，ｓ＿（ｎ－１））とし、Ｈ（Ｍ　||　Ｔ＿ｉ　||　Ｒ＿１）などとして第２の連鎖型署名データを作成する。公開時にはＲｅｐを秘匿しておき、Ｒ＿１と第２の連鎖型署名データを公開する。公開後に、否認署名を行いたいエンティティが登場したときにはじめて第１の連鎖型署名データとＲｅｐを公開し、第１の連鎖型署名データ、第２の連鎖型署名データそれぞれからα^*を算出して否認署名データの作成にもちいることが可能となる。

【０１０１】

［その他の実施形態］

本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体（または記憶媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本発明を構成することになる。

【０１０２】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１０３】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【０１０４】

本発明を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【０１０５】

以下に本発明の実施態様の例を示す。

【０１０６】

［実施態様１］　Ｎ個の公開鍵とそのうちの１つの公開鍵に対応する秘密鍵によって作成可能で、Ｎ個の公開鍵のそれぞれについて署名の検証が可能で、Ｎ人のメンバーのうち誰が署名したかを秘匿することのできる連鎖型署名において、前記連鎖型署名データの作成者以外のユーザが署名していないことを検証できるようにするための否認データを生成する手段を備えることを特徴とする連鎖型署名作成装置。

【０１０７】

［実施態様２］　メッセージにデジタル署名を施す際に、事前計算データをメッセージとともにハッシュ関数で圧縮するデジタル署名方式において、Ｎ個の公開鍵とそのうち少なくとも一つの秘密鍵を有し、第１の事前計算データを生成し、前記メッセージと第ｉの事前計算データを含むデータに対して第ｉのハッシュ値を計算するハッシュ計算手段と、

第ｉのハッシュ値に署名が施されたように見せかけるように第ｉの事前計算データと第ｉの署名データを擬似的に計算する擬似計算手段と、

前記擬似計算手段を逐次的に繰り返して得られた第Ｎのハッシュ値に対して、第１の事前計算データに呼応した第１の署名データを前記秘密鍵から生成する署名手段と

を備えることを特徴とする連鎖型署名作成装置。

【０１０８】

［実施態様３］　メッセージにデジタル署名を施す際にメッセージだけをハッシュ関数で圧縮してから演算を行うデジタル署名方式において、

該デジタル署名方式を、事前計算データを計算してメッセージとともにハッシュ関数で圧縮するデジタル署名方式に変更して実行することを特徴とする実施態様２に記載の連鎖型署名作成装置。

【０１０９】

［実施態様４］　実施態様２又は３に記載の連鎖型署名作成装置で生成された連鎖型署名データに対して、前記連鎖型署名データの作成者以外のユーザが署名していないことを検証できるようにするために、否認データを生成する手段を有することを特徴とする連鎖型署名作成装置。

【０１１０】

［実施態様５］　更に、

署名対象メッセージを受領する署名対象メッセージ受領手段と、

前記署名対象メッセージに対する連鎖型署名が施された連鎖型署名データを受領する連鎖型署名データ受領手段と、

前記署名対象メッセージに対して誓約データを付加する誓約データ付加手段と、

前記連鎖型署名データから署名の再計算に必要なデータを抽出する付随データ抽出手段と、

前記誓約データ付加手段で作成された誓約データ付加済みメッセージに対して改めて署名を施す再署名手段と、

前記再署名手段で計算されたデータを出力する否認データ出力手段とを備えることを特徴とする実施態様４に記載の連鎖型署名作成装置。

【０１１１】

［実施態様６］　前記再署名手段は、

前記誓約データ付加手段で得られたデータのハッシュ値を改めて計算するハッシュ再計算手段と、

前記ハッシュ再計算手段で計算されたハッシュ値に対して演算を施す演算手段と

を備えることを特徴とする実施態様５に記載の連鎖型署名作成装置。

【０１１２】

［実施態様７］　前記誓約データは事前計算データで代用することを特徴とする実施態様５に記載の連鎖型署名作成装置。

【０１１３】

［実施態様８］　前記第１の事前計算データは位数Ｐ－１の乗法群（ただしＰは素数）の生成元ｇに対して、擬似乱数ｋ（＜Ｐ－１）を生成し、ｇ＾ｋ（ｍｏｄ　Ｐ）の演算を行い、この演算結果を第１の事前計算データとすることを特徴とする実施態様２乃至７の何れか１項に記載の連鎖型署名作成装置。

【０１１４】

［実施態様９］　前記デジタル署名方式は離散対数問題に安全性を置くデジタル署名方式であることを特徴とする実施態様１乃至８の何れか１項に記載の連鎖型署名作成装置。

【０１１５】

［実施態様１０］　前記否認データは対話的なやり取りで証明することを特徴とする実施態様１乃至９の何れか１項に記載の連鎖型署名作成装置。

【０１１６】

［実施態様１１］　メッセージにデジタル署名を施す際に事前計算データをメッセージとともにハッシュ関数で圧縮するデジタル署名方式において、Ｎ個の公開鍵を有し、前記メッセージと第ｉの事前計算データを含むデータに対して第ｉのハッシュ値を計算するハッシュ計算手段と、

第ｉの署名データに検証のための演算を施す検証演算手段と、

前記検証演算手段を逐次的に繰り返して得られた第Ｎのハッシュ値が第１のハッシュ値と一致するかどうかを検証する検証手段と

を備えることを特徴とする連鎖型署名検証装置。

【０１１７】

［実施態様１２］　メッセージにデジタル署名を施す際にメッセージだけを

ハッシュ関数で圧縮してから演算を行うデジタル署名方式において、該デジタル署名方式を、事前計算データを計算してメッセージとともにハッシュ関数で圧縮するデジタル署名方式に変更して実行することを特徴とする実施態様１１に記載の連鎖型署名検証装置。

【０１１８】

［実施態様１３］　実施態様１乃至３の何れか１項に記載の連鎖型署名作成装置で生成された連鎖型署名データに対して、前記連鎖型署名データの作成者以外のユーザが署名していないことを検証できるようにするために否認データを生成する手段を更に備えることを特徴とする実施態様１１又は１２に記載の連鎖型署名検証装置。

【０１１９】

［実施態様１４］　更に、

署名対象メッセージを受領する署名対象メッセージ受領手段と、

前記署名対象メッセージに対する連鎖型署名が施された連鎖型署名データを受領する連鎖型署名データ受領手段と、

前記連鎖型署名データ受領手段に対する否認データを受領する否認データ受領手段と、

前記否認データに対応する誓約データを受領する誓約データ受領手段と、

前記連鎖型署名データから検証に必要なデータを抽出する付随データ抽出手段と、

前記署名対象メッセージ、上記誓約データからハッシュ値を計算するハッシュ演算手段と、

前記否認データに前記公開鍵で演算を施し、前記ハッシュ演算手段で得られたデータと一致するかどうかを検証する否認データ検証手段と

を備えることを特徴とする実施態様１３に記載の連鎖型署名検証装置。

【０１２０】

［実施態様１５］　前記デジタル署名方式は離散対数問題に安全性を置くデジタル署名方式であることを特徴とする実施態様１１乃至１４の何れか１項に記載の連鎖型署名検証装置。

【０１２１】

［実施態様１６］　前記否認データは対話的なやり取りで証明することを特徴とする実施態様１１乃至１５の何れか１項に記載の連鎖型署名検証装置。

【０１２２】

［実施態様１７］　実施態様１乃至８の何れかに記載の連鎖型署名作成装置と、実施態様１１乃至１６の何れかに記載の連鎖型署名検証装置とを有することを特徴とする連鎖型署名システム。

【０１２３】

［実施態様１８］　Ｎ個の公開鍵とそのうちの１つの公開鍵に対応する秘密鍵によって作成可能で、Ｎ個の公開鍵のそれぞれについて署名の検証が可能で、Ｎ人のメンバーのうち誰が署名したかを秘匿することのできる連鎖型署名において、前記連鎖型署名データの作成者以外のユーザが署名していないことを検証できるようにするための否認データを生成する工程を備えることを特徴とする連鎖型署名作成方法。

【０１２４】

［実施態様１９］　メッセージにデジタル署名を施す際に、事前計算データをメッセージとともにハッシュ関数で圧縮するデジタル署名方式において、Ｎ個の公開鍵とそのうち少なくとも一つの秘密鍵を有し、第１の事前計算データを生成し、前記メッセージと第ｉの事前計算データを含むデータに対して第ｉのハッシュ値を計算するハッシュ計算工程と、

第ｉのハッシュ値に署名が施されたように見せかけるように第ｉの事前計算データと第ｉの署名データを擬似的に計算する擬似計算工程と、

前記擬似計算工程における処理を逐次的に繰り返して得られた第Ｎのハッシュ値に対して、第１の事前計算データに呼応した第１の署名データを前記秘密鍵から生成する署名工程と

を備えることを特徴とする連鎖型署名作成方法。

【０１２５】

［実施態様２０］　メッセージにデジタル署名を施す際に事前計算データをメッセージとともにハッシュ関数で圧縮するデジタル署名方式において、Ｎ個の

公開鍵を有し、前記メッセージと第ｉの事前計算データを含むデータに対して第ｉのハッシュ値を計算するハッシュ計算工程と、

第ｉの署名データに検証のための演算を施す検証演算工程と、

前記検証演算工程における処理を逐次的に繰り返して得られた第Ｎのハッシュ値が第１のハッシュ値と一致するかどうかを検証する検証工程と

を備えることを特徴とする連鎖型署名検証方法。

【０１２６】

［実施態様２１］　コンピュータを実施態様１乃至１０の何れか１項に記載の連鎖型署名作成装置として機能させることを特徴とするプログラム。

【０１２７】

［実施態様２２］　コンピュータを実施態様１１乃至１６の何れか１項に記載の連鎖型署名検証装置として機能させることを特徴とするプログラム。

【０１２８】

［実施態様２３］　コンピュータに実施態様１８又は１９に記載の連鎖型署名作成を実行させることを特徴とするプログラム。

【０１２９】

［実施態様２４］　コンピュータに実施態様２０に記載の連鎖型署名検証方法を実行させることを特徴とするプログラム。

【０１３０】

［実施態様２５］　実施態様２１乃至２４の何れか１項に記載のプログラムを格納することを特徴とするコンピュータ読み取り可能な記憶媒体。

【０１３１】

【発明の効果】

以上説明したように、本発明によれば、勝手に流用された公開鍵に対する秘密鍵を保持するユーザ自らが署名していないことを示す（否認する）ことができない問題を解決し、ユーザが署名を作成していないことを示す否認データを作成することができる。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る連鎖型署名作成処理、連鎖型署名検証処理を実行する装置に適用するコンピュータの基本構成を示す図である。

【図２】

リング署名に対する否認データ作成処理を行うための装置の機能構成、もしくはこの処理をコンピュータに実行させるためのプログラムの機能構成を示す図である。

【図３】

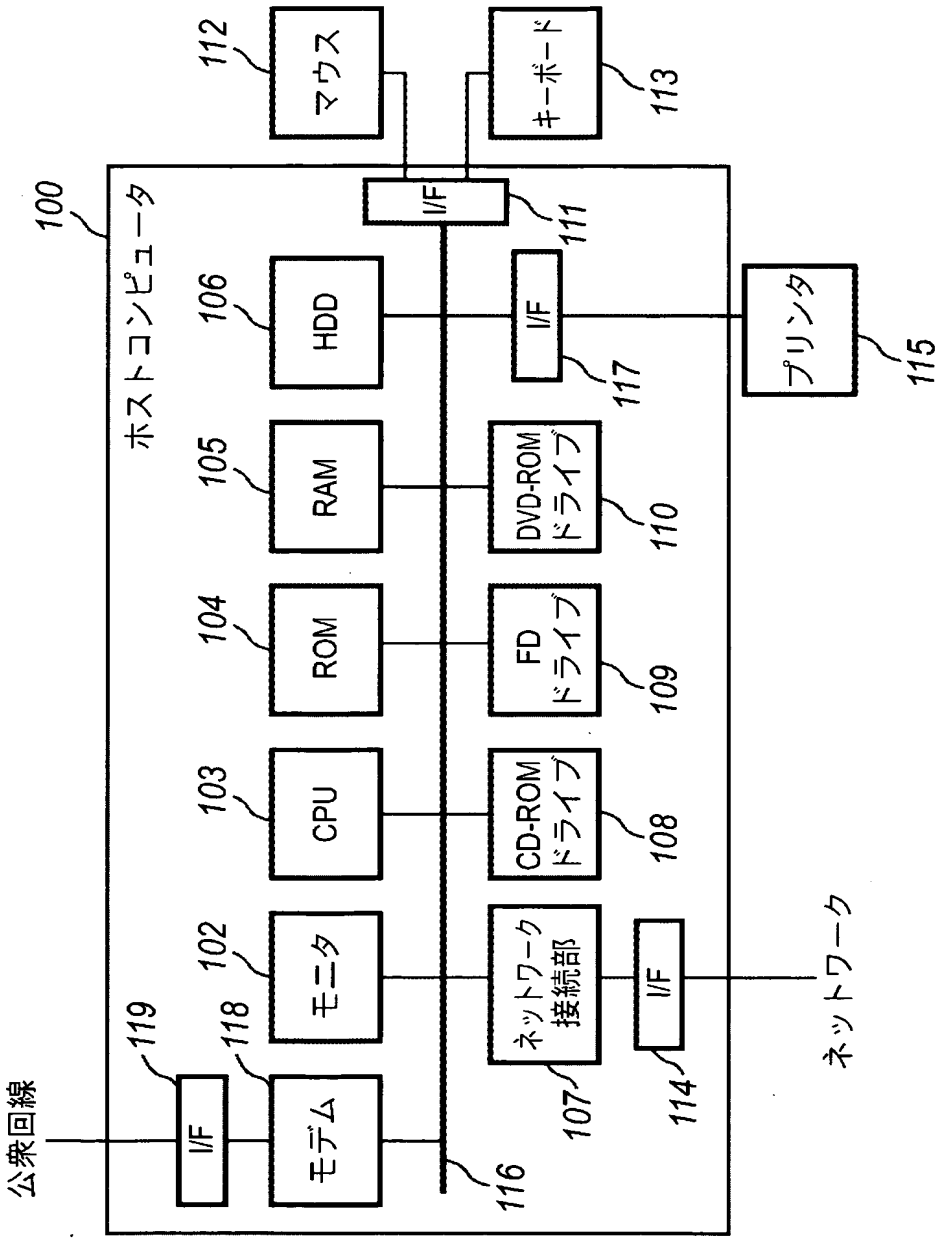
否認データを作成する処理のフローチャートである。

【図４】

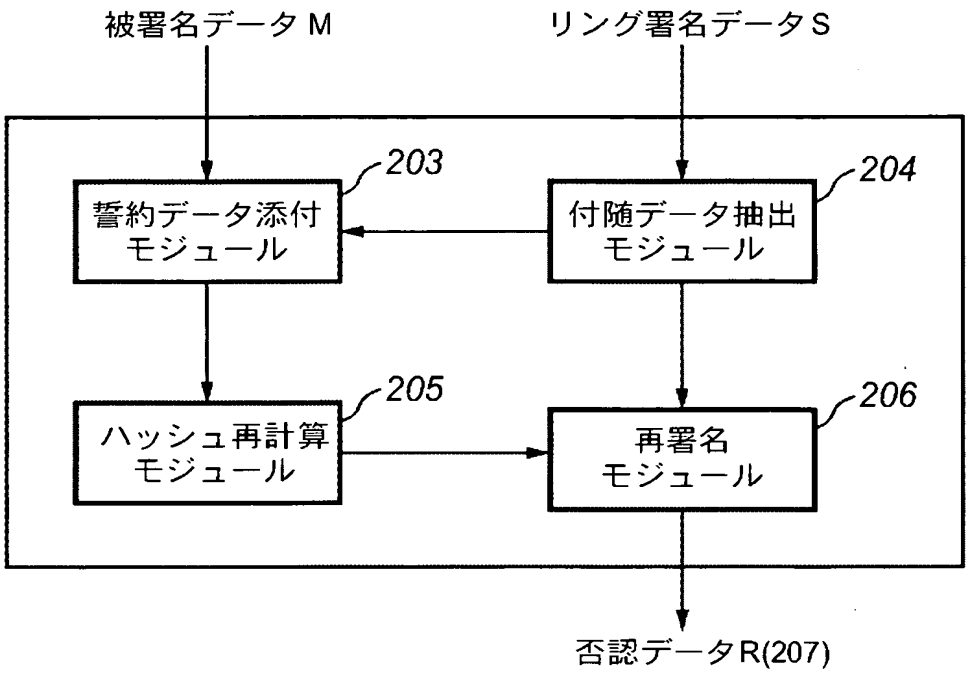
インタラクティブに否認するプロトコル処理を表す図である。

【書類名】　図面

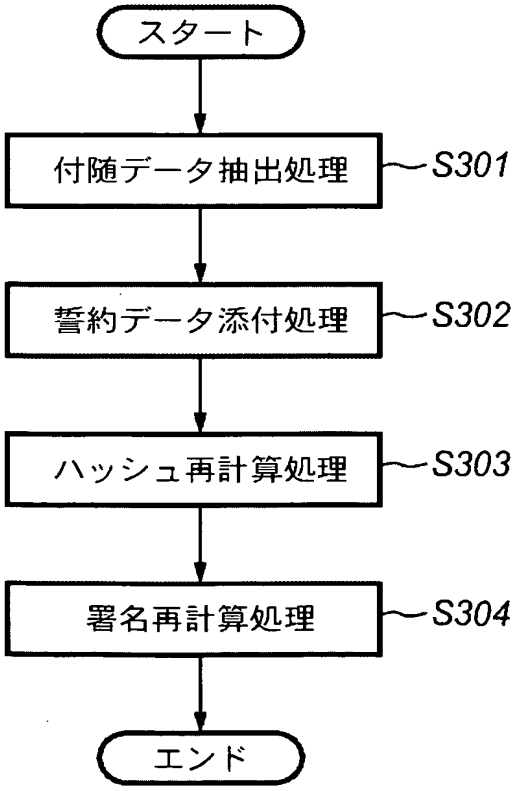
【図１】


100
ホストコンピュータ
112
マウス
113
キーボード
111
I/F
106
HDD
117
I/F
115
プリンタ
105
RAM
110
DVD-ROM ドライブ
104
ROM
109
FD ドライブ
103
CPU
108
CD-ROM ドライブ
102
モニタ
107
ネットワーク 接続部
114
I/F
ネットワーク
119
I/F
118
モデム
公衆回線
116

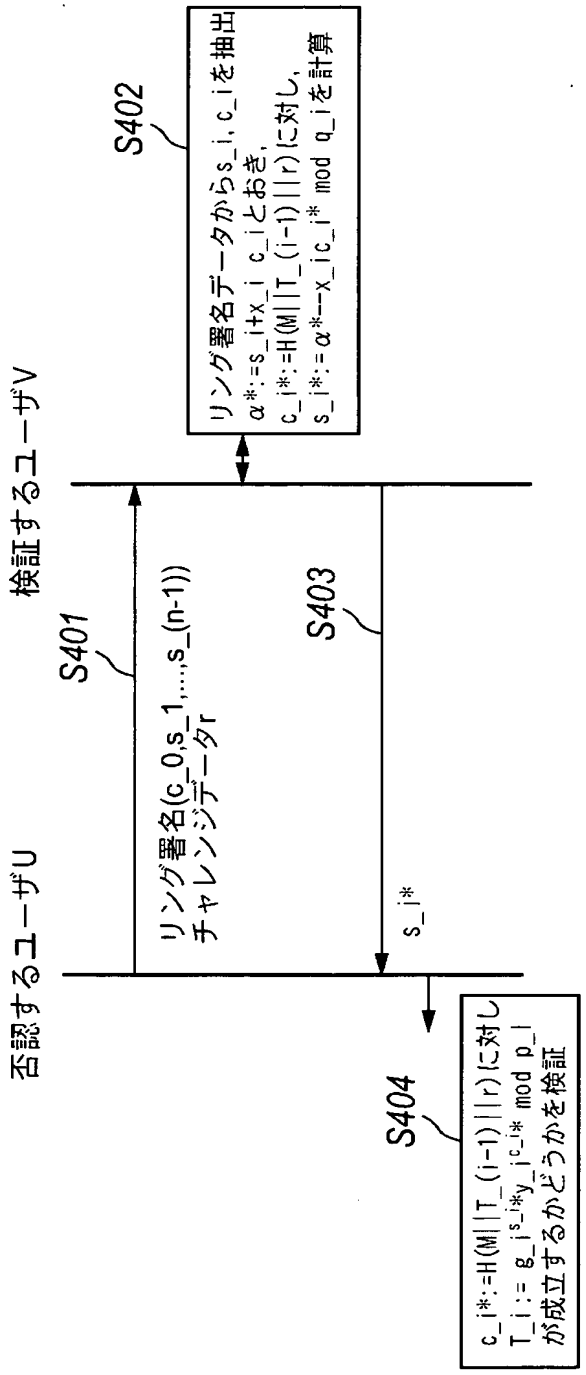
【図２】


被署名データＭ
リング署名データＳ
203
誓約データ添付
モジュール
204
付随データ抽出
モジュール
205
ハッシュ再計算
モジュール
206
再署名
モジュール
否認データR(207)

【図３】


スタート
付随データ抽出処理
S301
誓約データ添付処理
S302
ハッシュ再計算処理
S303
署名再計算処理
S304
エンド

【図４】


検証するユーザV
否認するユーザU
S401
リング署名(c_0,s_1,...,s_(n-1))
チャレンジデータr
S402
リング署名データからs_i, c_iを抽出
α*:=s_i+x_i c_iとおき,
c_i*:=H(M||T_(i-1)||r)に対し,
s_i*:=α*−x_ic_i* mod q_iを計算
S403
s_i*
S404
c_i*:=H(M||T_(i-1)||r)に対し
T_i:= g_i^s_i*y_i^c_i* mod p_i
が成立するかどうかを検証

【書類名】　要約書

【要約】

【課題】　連鎖型署名において、勝手に流用された公開鍵に対する秘密鍵を保持するユーザ自らが署名していないことを示す（否認する）ことができない問題を解決し、ユーザが署名を作成していないことを示す否認データを作成すること。

【解決手段】　モジュール２０４はリング署名データSからs_i,c_iを抽出し、s_i,c_i、秘密鍵x_iからα^*:=s_i+x_i c_iを計算する。被署名データMが入力され、同時にモジュール２０４においてT_(i-1)が抽出され、モジュール２０３はMにT_(I-1)と誓約データRepを付加し、モジュール２０５はc_i*:=H(M || T_(i-1) || Rep)を計算する。α^*,c_i*およびランダム値ｒに基づき、モジュール２０６はs_i*:= r － α^* c_i* mod q_iを計算し、否認データRを出力する。

【選択図】　図２

特願２００３－０１６７１８

出　願　人　履　歴　情　報

識別番号　［０００００１００７］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社